From Full-Custom to Fully-Standard Cell Power Analysis Countermeasures

Moshe Avital, Alexander Fish and Osnat Keren

Faculty of Engineering, Bar-Ilan University, Ramat-Gan 52900, Israel

e-mail:{moshe.avital, osnat.keren, alexander.fish }@ biu.ac.il

Extended Abstract

Side-Channel Analysis (SCA) attacks have become one of the most significant problems in modern digital systems. These attacks exploit and misuse the information related to the physical behavior of cryptographic devices such as power consumption, emitted electromagnetic radiation, etc. One of the most powerful SCA attacks is known as Power Analysis (PA). It does not require any assumptions regarding the hardware implementation of the cryptographic chip, a complex setup or unique measurement equipment. PA attacks target power supply monitoring, and fall into the category of *passive non-invasive* attacks. This paper presents three methods to counter PA attacks.

The first, called Randomized Multi-Topology Logic (RMTL), is a *full-custom* countermeasure that focuses on gate-level randomization. An RMTL gate can be configured dynamically to operate in one of several topologies, where each topology induces a different power profile. When embedding several RMTL gates in a crypto-system, the best protection against PA attacks is achieved by a random change between the topologies of each RMTL gate during run time. Security results examining the RMTL based implementation clearly show high immunity to PA attacks. However, like many other known hardware based full-custom countermeasures, implementing the RMTL gates and integrating them in a crypto-system requires considerable effort, and make it very difficult to commercialize this technology.

The second methodology focuses on embedding *CMOS based* gates, dubbed Blurring Gates (BG), into a crypto-system. This BG based technique is a *fully-standard cell* design: it is totally synthesizable and can be implemented with standard flow tools and libraries. Hence, its implementation is definitely much simpler. BG gates have two modes of operation: static and dynamic. They are placed along the logic path to distribute the propagation over the whole clock cycle period (or over a predefined part of it). Each BG can switch randomly between the two operational modes every cycle. This, in turn, blurs the information passed in a clock cycle over the entire cycle. The embedding configurations result in a powerful hardware technique with high immunity to PA attacks. Figure 1(a) illustrates a BG based implementation of a combinatorial logic. Figure 1(b) shows correlation results vs. time for all possible key guesses. As can be seen, the correct key cannot be revealed. However, the number of required random signals (derived from the number of the embedded BG units) requires an area overhead for routing and transferring the random signals from a True Random Number Generator (TRNG) module to the BG gates in a protected way.

The third methodology is a *fully-standard cell* design. Unlike the first and second countermeasures, in this technology the area used for routing and transferring random signals from the TRNG-generator to the BG gates is preserved but a different architecture to integrate the BG gates with the random signals is required.

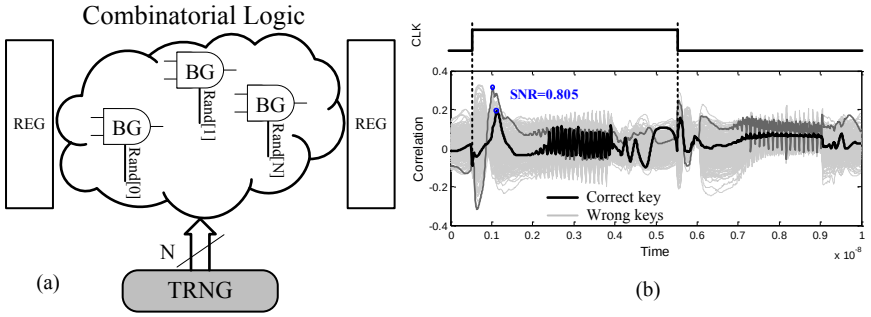

Figure 1 – (a) BG based countermeasure. (b) Correlation results of BG based 8-bit S-box (using 1000 input vectors).

***Category – poster presentation.**